Major Project Phase-Two

RSA vs ECC : A COMPARTIVE ANALYSIS

Department of Mathematics
GURU GHASIDAS VISHWAVIDYALAYA,
BILASPUR, (C.G.), INDIA.

Submitted in partial fulfilment of the requirements of the degree of

Master of Science

in

Mathematics

By

Ujjwal Kumar Garg
Roll No: 21075153
Enrolment No. GGV/21/05735

under the supervision of

Prof. P. P. Murthy

DECLERATION

I hereby declare that the entire work presented in the project work on **RSA vs ECC : A COMPARTIVE ANALYSIS** submitted for partial fulfillment of M.sc Mathematics has been performed in the Department of Mathematics Guru Ghasidas Vishwavidalaya, Bilaspur under the supervision of Prof. P.P. Murthy.
The work presented in this disseration is orignal and will remain intellectual property of Department of Mathematics, Guru Ghasidas Vishwavidalaya, Bilaspur(C.G).

Ujjwal Kumar Garg
M.sc. Mathematics
Roll No. 21075153

CERTIFICATE

This is to certify that the dissertation entitled "**RSA vs ECC : A COMPARTIVE ANALYSIS**" is based on a part of research work carried out by **Ujjwal Kumar Garg** under my guidance and supervision at Guru Ghasidas Vishwavidyalaya, Bilaspur,(C.G), 495009

.....
Prof. P. P. Murthy
Supervisor

.....
Dr. J. P. Jaiswal
H.O.D

Date: .....

ACKNOWLEDGEMENT

In the successful completion of this project, many people have bestowed upon me with their blessings and heartfelt support. This time, I am utilizing this opportunity to thank all the people who have been concerned with this project. I would thank God for allowing me to complete this project successfully. I would like to thank Head of Department Dr. J. P. Jaiswal, whose valuable support help througout this project. I express my gratidue to my supervisour Prof. P. P. Murthy for his stimulated discussion, crtical analysis and support from time to time. Last but not least I would like to thank my friends and research scholars of department who have helped me with their valuable suggestions and guidance has been very helpful in various phases of the project.

Ujjwal Kumar Garg

Contents

1 History

There have been **Three well-defined Phases** in the history of cryptology.

The **First phase** was the period of manual cryptography, starting with the origins of the subject in antiquity and continuing through World War I. This phase cryptography was limited by the complexity of what a code clerk could reasonably do aided by simple mnemonic devices. As a result, ciphers were limited to at most a few pages in size, i.e., to only a few thousands of characters.M General principles for both cryptography and cryptanalysis were known, but the security that could be achieved was always limited by what could be done manually. Most systems could be cryptanalyzed, therefore, given sufficient ciphertext and effort. One way to think of this phase is that any cryptography scheme devised during those two millennia could have equally well been used by the ancients if they had known of it.

The **Second Phase**, the mechanization of cryptography, began shortly after World War I and continues even today. The applicable technology involved either telephone and telegraph communications (employing punched paper tape, telephone switches, and relays) or calculating machines such as the Brunsvigas, Marchants, Facits, and Friedens (employing gears, sprockets, ratchets, pawls, and cams). This resulted in the rotor machines used by all participants in World War II.

The **Third Phase**, dating only to the last two decades of the 20th century, marked the most radical change of all—the dramatic extension of cryptology to the information age: digital signatures, authentication, shared or distributed capabilities to exercise cryptologic functions, and so on. It is tempting to equate this phase with the appearance of public-key cryptography, but that is too narrow a view. Cryptology's Third Phase was the inevitable consequence of having to devise ways for electronic information to perform all of the functions that had historically been done .

1.1 1920 B.C Egypt-Hieroglyph

It was used as early as 1900 BC in ancient Egypt. During these time the Egyptians would create a code using Hieroglyphics by switchings the order of them and only the people who knew the order could the translate the message
In this Hieroglyphic alphabets design like as sanke means the woerd "j" symbols likes the waves is stand for "n" and the same as the meaning of the all the symbol.

Figure 1:

1.2 1500 B.C Babylonian

The lenticular clay tablet was used to help scribes learn to write the sumerian and Akkadian languages using the triangle-like cuneiform script.To learn a word or sign,the teacher would write the form on the obverse,and the student would then repeat the excerise on the revrse.Such elementry excerise were often completed on the tablets that were smalland round,easily fitting into the plam of hand
On this tablet,the name of the deity Urash was copied six times.(Additional signs seem to be present on the reverse but are too damaged to read).Two signs used to write this name:the first star-like sign on the left is a sign thst was used the indicate the name ofa for Urash ,the name of diety. cuneiform writing,therefore,requried the mastery of sevral hundred sign and their diffrent meaning.A Babyloian cuneiform tablet ,dating from about 1500 BC,contains

an encrypted recipe for making pottery glaze.This example more likely represents the occurence of ciphers in this part of the world as this would be fairly trivial.

Figure 2:

1.3 58 B.C. Julius-Ceaser

The first important use of cryptography is the reloctation code.This was described by the greek writer polyibus as a substitution technique but his military use was developed by the Roman Emperor Julius ceasar(58BC).Caesar communicated with his commanders through this encryption method. messages are replacing the letter in the text with one of the three position to the right. For example,the word ENDER was changed to HQGHU.

1.4 5 B.C. Spatra

In the 5th century BC,the first displacment system was introduced by a method developed by sparta.For this reason,the first nation to use cryptography in military communicartrion is referred to as sparta.The developed

device consisted of a wooden roller of a certain thickness and a papryus or a thin, leather band that was bent around the cylinder. the hidden message was written over the roll along the roll,and then the strip was unwound ffrom the cylinder and transmitted to the desired traget. Here ,the diameter of the cylinder served as a key to the encryption and resoulation of the text.

1.5 History of Enigma

The **History of the Enigma** starts **around 1915**, with the invention of the rotor-based cipher machine. As usual in history, the rotor machine was invented more or less simultaneously in different parts of the world. In 1917 there were inventions from Edward Hebern in the USA, Arvid Damm in Sweden, Hugo Koch in The Netherlands and Arthur Scherbius in Germany

An Enigma machine is a famous encryption machine used by the Germans during (WWII) to transmit coded messages. An Enigma machine allows for billions and billions of ways to encode a message, making it incredibly difficult for other nations to crack German codes during the war — for a time the code seemed unbreakable. The Enigma machine was invented by Arthur Scherbius in 1918, right at the end of World War I. After several years of improving his invention, the first machine saw the light of day in 1923. A year earlier he had secured the rights to patent NL10700 of Dutch inventor Hugo Koch for a similar device.

The Enigma machine, which combined electrical and mechanical components, was descended from a number of designs that were submitted for patent as early as 1918 in Germany and were produced commercially beginning in the early 1920s. Looking rather like a typewriter, it was battery-powered and highly portable. In addition to a keyboard, the device had a lamp board consisting of 26 stenciled letters, each with a small lightbulb behind it. As a cipher clerk typed a message on the keyboard in plain German, letters were illuminated one by one on the lamp board. An assistant recorded the letters by hand to form the enciphered message, which was then transmitted in Morse Code.Each bulb in the lamp board was electrically connected to a letter on the keyboard, but the wiring passed via a number of rotating wheels, with the result that the connections were always changing as the wheels moved. Thus, typing the same letter at the keyboard, such as AAAA..., would produce a stream of changing letters at the lamp board, such as WMEV.... It was this ever-changing pattern of connections that made Enigma extremely hard to break.

The earliest success against the German military Enigma was by the Pol-

Figure 3:

ish Cipher Bureau. In the winter of 1932–33, Polish mathematician Marian Rejewski deduced the pattern of wiring inside the three rotating wheels of the Enigma machine. (Rejewski was helped by photographs, received from the French secret service, showing pages of an Enigma operating manual for September and October 1932.) Before an Enigma operator began enciphering a message, he set Enigma's three wheels (four in models used by the German navy) to various starting positions that were also known to the intended recipient. In a major breakthrough, Rejewski invented a method for finding out, from each intercepted German transmission, the positions in which the wheels had started at the beginning of the message. In consequence, Poland was able to read encrypted German messages from 1933 to 1939. In the summer of 1939 Poland turned over everything—including information about Rejewski's Bomba, a machine he devised in 1938 for breaking Enigma messages—to Britain and France. In May 1940, however, a radical change to the Enigma system eliminated the loophole that Rejewski had exploited to discover the starting positions of the wheels.

"Cryptography without system integrity is like investing in an armored car to carry money between a customer living in a cardboard box and a person doing business on a park bench." — **Gene Spafford**

2 Cryptography

Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents. The term is derived from the Greek word kryptos, which means hidden. It is closely associated to encryption, which is the act of scrambling ordinary text into what's known as ciphertext and then back again upon arrival. In addition, cryptography also covers the obfuscation of information in images using techniques such as microdots or merging. Ancient Egyptians were known to use these methods in complex hieroglyphics, and Roman Emperor Julius Caesar is credited with using one of the first modern ciphers.

2.1 Definitions

Cryptography is the process of hidding or coding of information so that only the person a message was intended for can read it. The art of cryptography has been used to code messages for thousands of years and continues to be used in bank cards, computer passwords, and ecommerce.

A common cryptography definition is the practice of coding information to ensure only the person that a message was written for can read and process the information. This cybersecurity practice, also known as cryptology, combines various disciplines like computer science, engineering, and mathematics to create complex codes that hide the true meaning of a message.

Cryptography is the study and practice of techniques for secure communication in the presence of third parties called adversaries. It deals with developing and analyzing protocols which prevents malicious third parties from retrieving information being shared between two entities thereby following the various aspects of information security

"A cryptographic system should be secure even if everything about the system, except the key, is public knowledge." — **Auguste Kerckhoffs**

2.2 Importance of Cryptography

Cryptography is an essential information security tool. It provides the four most basic services of information security

- **Confidentiality** : Encryption technique can guard the information and communication from unauthorized revelation and access of information.
- **Authentication** : The cryptographic techniques such as MAC and digital signatures can protect information against spoofing and forgeries.
- **Data Integrity** : The cryptographic hash functions are playing vital role in assuring the users about the data integrity.
- **Non-repudiation** : The digital signature provides the non-repudiation service to guard against the dispute that may arise due to denial of passing message by the sender.

All these fundamental services offered by cryptography has enabled the conduct of business over the networks using the computer systems in extremely efficient and effective manner.

"Cryptography without system integrity is like investing in an armored car to carry money between a customer living in a cardboard box and a person doing business on a park bench." — **Gene Spafford**

2.3 Terminology;

- **Plain Text:** It is usually a ordinary readble text.
- **Cipher Text:** Cipher text is encrypted text tranform from plain text using encryption algorithm.
- **Encryption:** Encryption is a process which transforms the original information into an unrecognizable form. This new form of the message is entirely different from the original message
- **Decryption:** Decryption is the process of converting an encrypted message back to its original format that is plain text.
- **Key:** A key is a string of characters used within an encryption algorithm for altering data so taht apperas random.

2.4 Types of Cryptography

1. Symmetric Key Cryptography

Symmetric key encryption, also called private key cryptography, is an encryption method where only one key is used to encrypt and decrypt messages. This method is commonly used in banking and data storage applications to prevent fraudulent charges and identity theft as well as protect stored data. A sender and their designated recipients have identical copies of the key, which is kept secret to prevent outsiders from decrypting their messages. The sender uses this key to encrypt their messages through an encryption algorithm, called a cipher, which converts plaintext to ciphertext. The designated recipients then use the same key to decrypt the messages by converting the ciphertext back to plaintext.

Categories of Symmetric Key Encryption

- **Data Encryption Standard (DES):** It was developed in the early 1970s and is considered a legacy encryption algorithm. This block cipher used 56-bit keys and encrypted block sizes of 64 bits. Due to its short key length, the encryption standard was not very secure. However, it played a vital role in the advancement of cryptography. Because

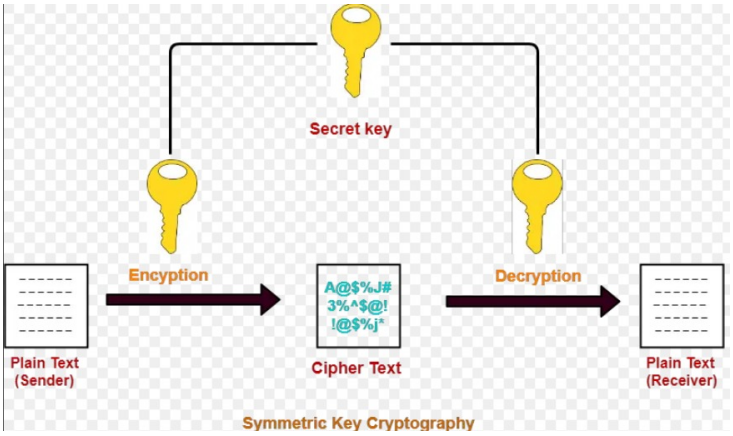


Figure 4:

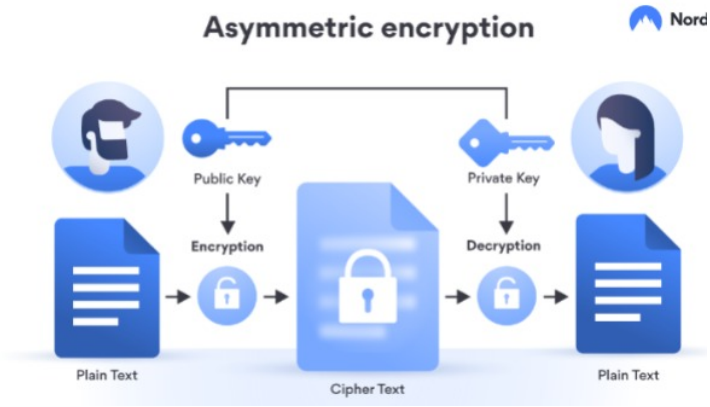
the US National Security Agency (NSA) participated in DES's development, many academics were skeptical. This skepticism caused a surge in cryptography research, which led to the modern understanding of block ciphers.

- **Advanced Encryption Standard (AES:)** It also known as Rijndael, supersedes DES. AES is an encryption standard used by the US government to encrypt classified information. It is also popular with companies such as Google, Mozilla, and Microsoft. It is a family of block ciphers developed by the Belgian cryptographers Vincent Rijmen and Joan Daemen. The AES family can handle block sizes and encryption key sizes of 128, 160, 192, 224, and 256 bits. Officially, only 128-, 192-, and 256-bit key sizes and a 128-bit block size are specified in the encryption standard.

"Every secret creates a potential failure point." — **Bruce Schneier**

2.Asymmetric Key Cryptography

Asymmetric cryptography is also called public key cryptography because it consists of two keys one is public key and second is private key.One key is used for encryption and the other key should be used for decryption. A public key is a cryptographic key that can be used by any person to encrypt a message so that it can only be decrypted by the intended recipient with their private key. A private key – also known as a secret key - is shared only with key's initiator.here is no other key can decrypt the message and not even the initial key used for encryption. The style of the design is that every communicating party needs only a key pair for communicating with any number of other communicating parties.
Asymmetric cryptography is scalable for use in high and ever expanding environments where data are generally exchanged between different communication partners. Asymmetric cryptography is used to exchange the secret key to prepare for using symmetric cryptography to encrypt information.
In the case of a key exchange, one party produce the secret key and encrypts it with the public key of the recipient. The recipient can decrypt it with their private key. The remaining communication would be completed with the secret key being the encryption key. Asymmetric encryption is used in key exchange, email security, Web security, and some encryption systems that needed key exchange over the public network.



3 RSA

RSA is considered as the first real life and practical asymmetric-key cryptosystem. It becomes de facto standard for public-key cryptography. Its security lies with integer factorization problem. RSA's decryption process is not efficient as its encryption process. Many researchers have proposed to improve the efficiency of RSA's decryption using Chinese Remainder Theorem (CRT).

RSA algorithm was presented by a group of a security researchers, Ronald Rivest, Adi Shamir, and Leonard Adleman. The term RSA was derived from the names of the three developers of this algorithm. Till now, RSA is most widely used as a public key cryptographic algorithm.

3.1 Algorithim

The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is a multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So if somebody can factorize the large number, the private key is compromised. Therefore encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially.

Key Generation

- Step I. Select p and q, where p and q both are prime numbers, p not equal to q
- Step II. Calculate n = pq
- Step III. Calculate ϕ(n) = $(p-1)(q-1)$
- Step IV. Select integer e such that 1< e< ϕ(n) ; gcd(ϕ(n),e) = 1
- Step V. Calculate d ; ed = mod (ϕ(n))
- Step VI. Public key pair = (n , e)
- Step VII. Private key pair = (n , d)

Encryption

- Step I. Plaintext: M $<$ n, where M is a plain text
- Step II. Ciphertext: $C = M^e \mod n$

Decryption

- Step I. Ciphertext: C
- Step II. Plaintext M $= C^d \mod n$

3.2 Security of RSA

There are three main approaches of attacking RSA algorithm.

Brute force key search (infeasible given size of numbers) As explained before, involves trying all possible private keys. Best defense is using large keys.

Mathematical attacks (based on difficulty of computing ϕ(N), by factoring modulus N) There are several approaches, all equivalent in efect to factoring the product of two primes. Some of them are given as:

factor $N = p * q$, hence find ϕ(N) and then d

determine ϕ(N) directly and find d

find d directly

The possible defense would be using large keys and also choosing large numbers for p and q, which should differ only by a few bits and are also on the order of magnitude 1075 to 10100.

3.3 Encryption and Decryption of plaintext

- Choose two prime numbers p and q where p = 7 and q = 17
- Now calculate n = $p * q$ = $7 * 17$=119
- Calculate ϕ(n) = (p - 1)(q - 1) = $(7-1)(17-1)$
  $6 * 16 = 96$
- Since the factors of 96 are $2*2*2*2*2*3$ therefore e select such that none of the factor of e as 2 and 3
- Let us choose e = 5
- Now we have a public key pair = (n , e) = $(5, 119)$
- Calcuation of d
  ed=mod ϕ(n)=1 so we get
  d = 77
- private key pair = (n , d) = (119 , 77)

3.4 Encryption of plaintext:

- Let m is our plaintext and m = 10
- the public key for encryption of plaintext is
  c = m^e mod (n)
  c=10^5 mod (119)
  c = 100000 mod(119)
  c = 40
  c = 40 is our ciphertext

3.5 Decryption of Ciphertext:

- the private key for decryption of plaintext is
  m = c^d mod (n)
- m = 40^{77} mod (119)
  m = 10

4 ECC

4.1 Histroy of ECC

The properties and function of elliptic curves in mathematics have been studied for more than 1500 years. Their use within cryptography was first proposed in 1985, separtly by Neal Koblitz from the university of Washington and Victor Miller at IBM.
They are the elliptic curves analogues if scheme based on the discrete logrith problem , where the underlying group is the group of points on an elliptic curve defined over a finite field.

4.2 Elliptic Curves Cryptography

The principal attraction of ECC compared to RSA is that it offers equal security for a far smaller key size, thereby reducing processing overhead. The addition operation in ECC is the counterpart of modular multiplication in RSA, and multiple addition is the counterpart of modular exponentiation. To form a cryptographic system using elliptic curves, we need to find a "hard problem". All systems rely on the difficulty of a mathematical problem for their security. To explain the concept of difficult mathematical problem, the notion of an algorithm is required. To analyze how long an algorithm takes, computer scientists introduced the idea of polynomial time algorithms and exponential time algorithms. An algorithm runs quickly if it is polynomial time algorithm, and slowly if it is exponential time algorithm. Therefore, easy problems equate with polynomial time algorithms, and difficult problems equate with exponential time algorithms. When looking for a mathematical problem on which to base a public key cryptographic system, cryptographers search for a problem for which the fastest algorithm takes exponential time. The longer it takes to compute the best algorithm for a problem, the more secure a public key cryptosystem based on that problem will be

The Elliptic Curve Cryptosystem, whose security rests on the discrete logarithm problem over the points on the elliptic curve. The main attraction of ECC over RSA and DSA is that the best known algorithm for solving the underlying hard mathematical problem in ECC (the elliptic curve discrete logarithm problem (ECDLP) takes full exponential time.

• **Definition:**

An elliptic curve is the set of points that satisfy a specific mathematical equation.
For ECC, we are concerned with a restricted form of elliptic curve that is defined over a finite field. Of particular interest for cryptography is what is referred to as the elliptic group mod p, where p is a prime number. This is defined as follows. Choose two nonnegative integers, a and b, less than p that satisfy:

$$4a^3 + 27b^2 \neq 0 \mod p$$

Then $E_q(a, b)$ denotes the elliptic group mod p whose elements (x, y) are pairs of nonnegative integers less than p satisfing :

$$y^2 = x^3 + ax + b$$

• The elliptic curve discrete logarithm problem can be stated as follows. Fix a prime p and an elliptic curve.

$$Q = xP$$

where xP represents the point P on elliptic curve added to itself x times. Then the elliptic curve discrete logarithm problem is to determine x given P and Q. It is relatively easy to calculate Q given x and P, but it is very hard to determine x given Q and P.

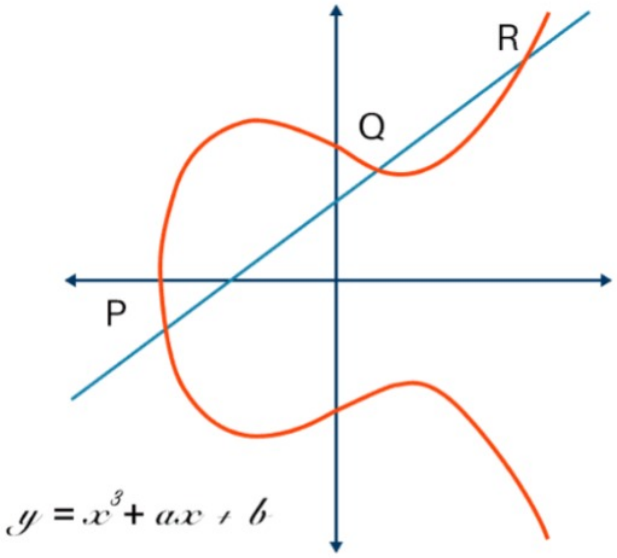


Figure 5:

4.3 Algorithm

- **Global Public Elements:**
  - Step I. $E_q(a, b)$ elliptic curve with parameters a, b, and q, where q is a prime or integer of the form 2^m.
  - Step II. G point on elliptic curve whose order is large value n
- **User A Key Generation:**
  - Step I. Select private key $n_A; n_A < n$
  - Step II. Calculate public key P_A
  - Step III. $P_A = n_A * G$
- **User B Key Generation:**
  - Select Private key $\mathrm{n}_B; n_B < nCalculatePublickey\mathrm{P}_B$
  - $P_B = n_B * G$

- **Calculation of Secret Key by User A:**
  - Step I. $K = n_A * P_B$
- **Calculation of Secret Key by User B:**
  - Step I. $K = n_B P_A$
- **Encryption by A using B Public Key:**
  - A chooses message P_m and a random positive integer k
  - Ciphertext $C_M = KG, P_M + kP_B$
- **Decryption by B using his own Private Key:**
  - Ciphertext: C_m
  - $P_M + kP_B - kG * n_B = P_M$

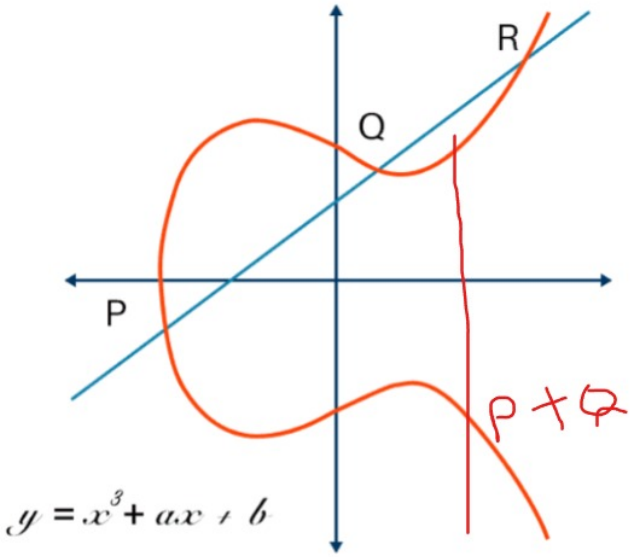


Figure 6: elliptic curve

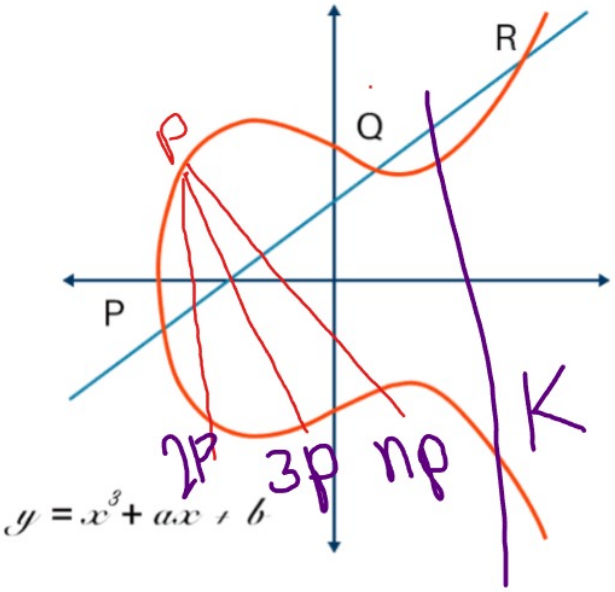


Figure 7:

- **Calculation of P+Q:**
- Let $P = (x_1, y_1)$ and$Q = (x_2, y_2)$
- And let $P + Q = (x_3, y_3)$
- $x_3 = \lambda^2 - x_1 - x_2$
- and $y_3 = \lambda(x_1 - x_3) - y_1 mod p$

- Where $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$

- **Calculation of $2P$:**
- Let P = Q then 2P equal to
- $\lambda = \dfrac{3x_1^2 + a}{2y_1}$ $x_3 = \lambda^2 - x_1 - x_2$
- $y_3 = \lambda(a\text{-}x_3) - y$

4.4 Problem on ECC

- **Global parameter of ECC are:**

Here prime number $p = 11, a = 1, b = 1$ for encoding and decoding of message in ellptic curve. Based on global parameters, the ellptic curve equations become:

$$y^2 \mod 11 = (x^3 + x + 1) \mod 11$$

GF(11)	$y^2 mod 11$	$x^3 + 2x + 1 mod 11$
0	0	1
1	1	3
2	4	0
3	9	3
4	5	3
5	3	10
6	3	3
7	5	10
8	9	4
9	4	2
10	1	10

- Step: 1 Encoded a plain text message as a point on the curve
  Lets consider the point to be encoded plain text message on the curve

$$M \in E_{11}(1, 1) is (4, 6)$$

- Step: 2 Eastablish the Public key and Privte key
  Chose a generator point

$$G \in E_{11}(1, 1)$$

let G is

$$(1, 5) \in E_{11}(1, 1)$$

Select a private key $n = 2$

Compute the Public key as $P_A = nG$

- Let nG equal to $(x_3, y_3) \mod 11$as $n = 2$ and $G = (1, 5)$
- $P_A = 2G = G + G = (1, 5) + (1, 5)$
- Let $x_1 = x_2 = 1$ and $y_1 = y_2 = 5$
- $\lambda = \frac{3x^2 + a}{2y_1} \mod 11 \ \frac{3 * 1^2 + 1}{2 * 5} \mod 11 = 7$
- $x_3 = \lambda^2\text{-x}_1 - x_2 \mod 11 = 7^2 - 1 - 1 \mod 11 = 3$
- $\text{y}_3 = \lambda(\text{a-x}_3) - \text{y} \mod 11 = 7(1 - 3) - 5 \mod 11 = 3$
- $\text{y}_3 = \lambda(\text{a-x}_3) - \text{y} \mod 11 = 7(1 - 3) - 5 \mod 11 = 3$
- now we have $(x_3, y_3) = (3, 3)$

- **Step:3 Encrypt the message using Public key**
- $C = [kG, M + kP_A]$ where k is a random number
- $C = [C_1, C_2]$
- Let $k = 2$

$C = [2(1, 5), (4, 6) + 2(3, 3)]$

$C = [(1, 5) + (1, 5), (4, 6) + (3, 3) + (3, 3)]$

$C = [(3, 3), (4, 6) + (3, 3) + (3, 3)]$

$C = [(3, 3), (4, 6) + (6, 5)]$

$C = [(3, 3), (4, 5)]$

$C_1 = (3, 3)$ and $C_2 = (4, 5)$

- **Step:4 Decrypt using private key:**

$M = C_2 - [nC_1]$

$M = (4, 5) - [2(3, 3)]$

$M = (4, 5) - [(3, 3), (3, 3)]$

$M = (4, 5) - (6, 5)$

$M = (4, 5) + (6, -5)$

$\lambda = \dfrac{y_2 - y_1}{x_2 - x_1} \mod 11 = \dfrac{-5 - 5}{6 - 4} \mod 11 = \text{-5} \mod 11 = 6$

$x_3 = \lambda^2 - x_1 - x_2 \mod 11 = 6^2 - 4 - 6 \mod 11 = 26 \mod 11 = 4$

$y_3 = \lambda(\mathrm{x}_1 - x_3)\text{- } \mathrm{y}_1 \mod 11 = 6(4 - 4) - 5 \mod 11 = 6$

$(x_3, y_3) = (4, 6)$

4.5 Analysis of RSA vs ECC

- 8 bits – Encryption and Decryption

Security bit level	ECC Enc. Time	RSA Enc. Time	ECC Dec. Time	RSA Dec. Time
80	0.4885	0.0307	1.3267	0.7543
112	2.2030	0.0299	1.5863	2.7075
128	3.8763	0.0305	1.7690	6.9409
144	4.7266	0.0489	2.0022	13.6472

- 64 bits – Encryption and Decryption

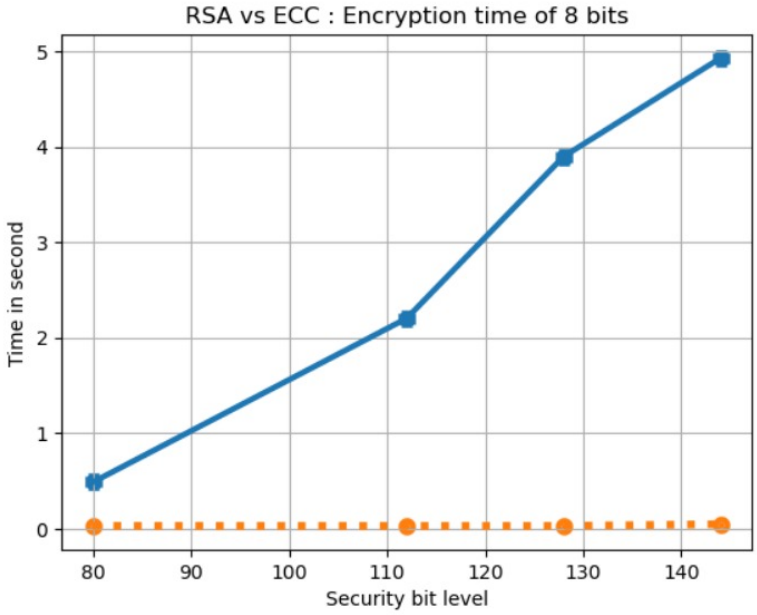
Security bit level	ECC Enc. Time	RSA Enc. Time	ECC Dec. Time	RSA Dec. Time
80	2.1685	0.1366	5.9099	5.5372
112	9.9855	0.1635	6.9333	20.4108
128	15.0882	0.1672	7.3584	46.4782
144	20.2308	.01385	8.4785	77.7642

- 256 bits – Encryption and Decryption

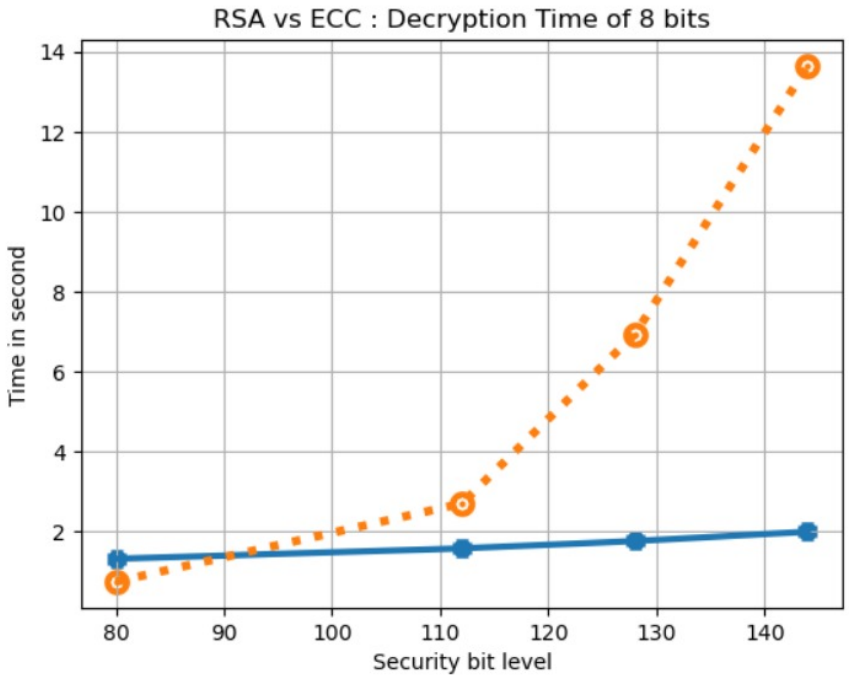
Security bit level	ECC Enc. Time	RSA Enc. Time	ECC Dec. Time	RSA Dec. Time
80	7.9240	0.5596	22.8851	19.3177
112	39.7008	0.5815	26.3331	102.0337
128	58.4386	0.5611	27.4060	209.6086
144	77.5034	0.5718	32.1522	311.0649

- x = [80,112,128,144]
- y=[.4885,2.2030,3.8963,4.9266]
- z=[0.0307,0.0299,0.0305,0.0489]
- plt.plot(x,y , linewidth = 3)
- plt.plot(x,z , linewidth =4)
- plt.scatter(x,y , marker="+" , linewidth=9)
- plt.scatter(x,z , marker = "." ,linewidth=9)
- plt.title("RSA vs ECC : Encryption time of 8 bits")
- plt.xlabel("RSA vs ECC : Ecryption Time of 8 bits")
- plt.ylabel("Time in second")
- plt.grid("true")
- plt.show()

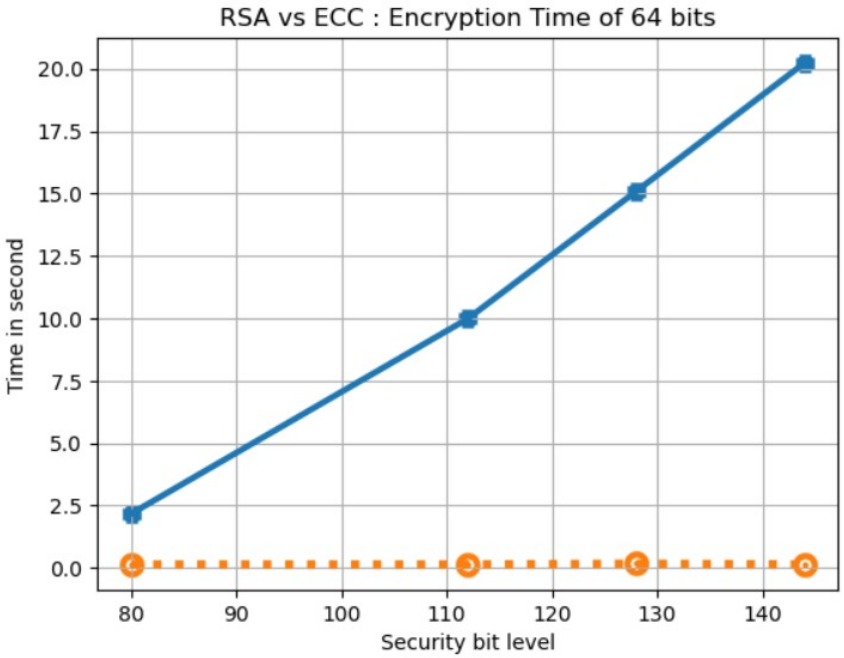
plain Line = ECC, Point Line = RSA



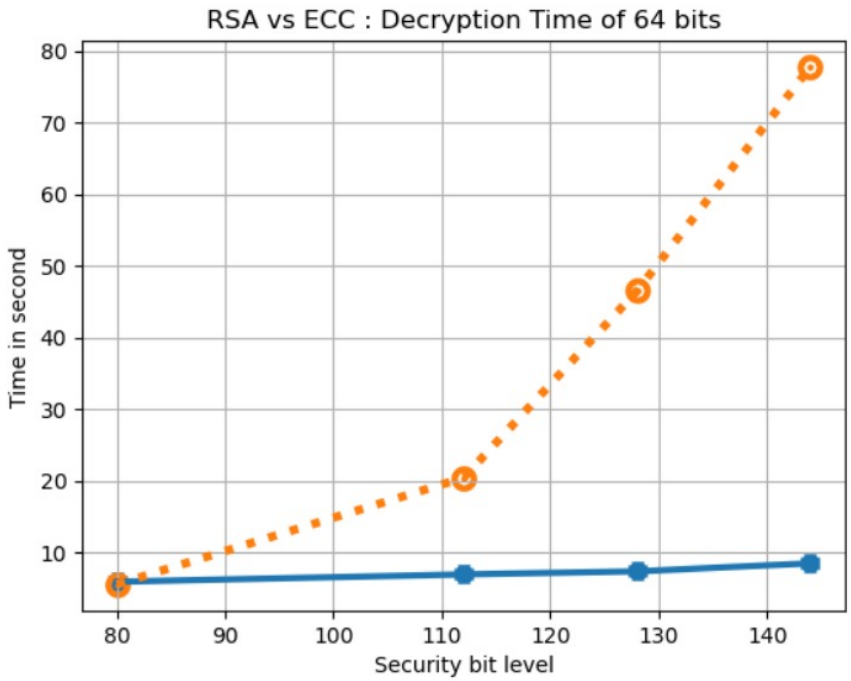
- x = [80,112,128,144]
- y1 = [1.3267,1.5863,1.7690,2.0022]
- z1 = [0.7543,2.7075,6.9409,13.6472]
- plt.plot(x,y1 , linewidth=3)
- plt.plot(x,z1 , linewidth=4)
- plt.scatter(x,y1,marker="+" , linewidth=9)
- plt.scatter(x,z1,marker=".",linewidth=9)
- plt.title("RSA vs ECC : Decryption Time of 8 bits")
- plt.xlabel("Security bit level")
- plt.ylabel("Time in second")
- plt.grid("true")
- plt.show()



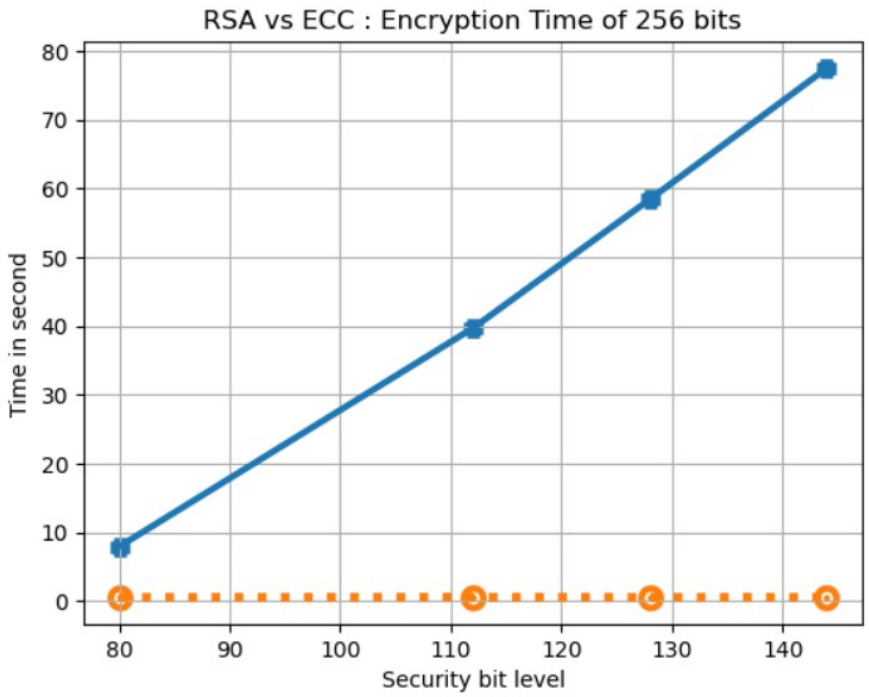
- x = [80,112,128,144]
- y2 = [2.1685 ,9.9855 ,15.0882 ,20.2308]
- z2= [0.1366 ,0.1366 ,0.1672 ,0.1385]
- plt.plot(x,y2 , linewidth=3)
- plt.plot(x,z2 , linewidth=4)
- plt.scatter(x,y2,marker="+" , linewidth=9)
- plt.scatter(x,z2,marker=".",linewidth=9)
- plt.title("RSA vs ECC : Encryption Time of 64 bits")
- plt.xlabel("Security bit level")
- plt.ylabel("Time in second")
- plt.grid("true")
- plt.show()



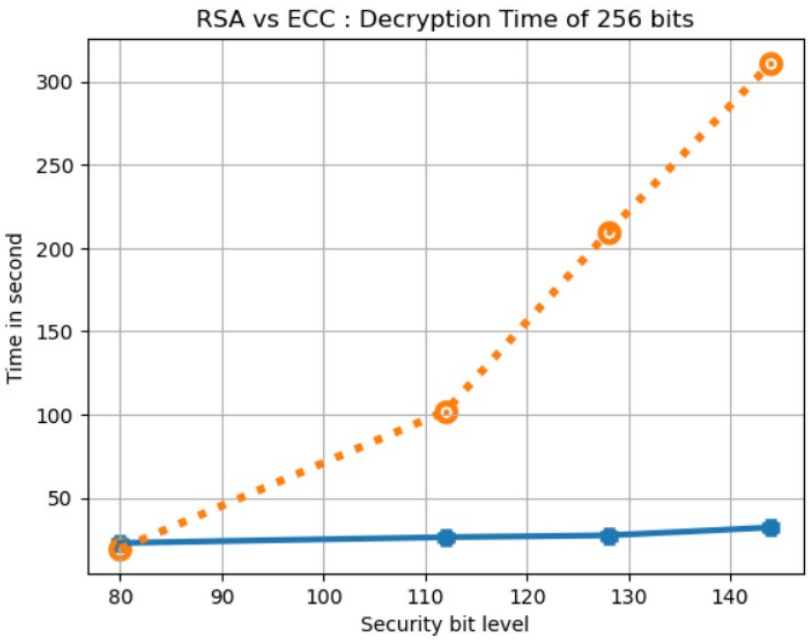
- x = [80,112,128,144]
- y3 = [5.9099,6.9333,7.3584,8.4785]
- z3 = [5.5372,20.4108,46.4782,77.7642]
- plt.plot(x,y3 , linewidth=3)
- plt.plot(x,z3 , linewidth=4)
- plt.scatter(x,y3,marker="+" , linewidth=9)
- plt.scatter(x,z3,marker=".",linewidth=9)
- plt.title("RSA vs ECC : Decryption Time of 64 bits")
- plt.xlabel("Security bit level")
- plt.ylabel("Time in second")
- plt.grid("true")
- plt.show()



- x = [80,112,128,144]
- y4 = [7.9240,39.7008,58.4386,77.5034]
- y4 = [7.9240,39.7008,58.4386,77.5034]
- plt.plot(x,y4 , linewidth=3)
- plt.plot(x,z4 , linewidth=4)
- plt.scatter(x,y4,marker="+" , linewidth=9)
- plt.scatter(x,z4,marker=".",linewidth=9)
- plt.title("RSA vs ECC : Encryption Time of 256 bits")
- plt.xlabel("Security bit level")
- plt.ylabel("Time in second")
- plt.grid("true")
- plt.show()



- x = [80,112,128,144]
- y5 = [22.8851,26.3331,27.4060,32.1522]
- z5 = [19.3177,102.0337,209.6086,311.0649]
- plt.plot(x,y5 , linewidth=3)
- plt.plot(x,z5 , linewidth=4)
- plt.scatter(x,y5,marker="+" , linewidth=9)
- plt.scatter(x,z5,marker=".",linewidth=9)
- plt.title("RSA vs ECC : Decryption Time of 256 bits")
- plt.xlabel("Security bit level")
- plt.ylabel("Time in second")
- plt.grid("true")
- plt.show()



4.6 Advantages of ECC over RSA

- ECC, it takes one−sixth the computational effort to provide the same level of cryptographic security that you get with 1024 bit RSA and is 15

Symmetric Encryption Key size in bits	RSA and DH key size	ECC key size
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

- Because of much smaller key sizes involved, ECC algorithm can be implemented on smartcards. Contactless smart cards work only with ECC
- ECC has become important for wireless sensor networks.
- ECC also serving as the standard mode of encryption that is used widely by various web applications.
- Poplur cryptocurrencies such as Bitcoin and Ethereum make use of the Elliptic Curve Digital Signature Algorithim particularly in signing transactions due to the security levels offered by ECC.

CONCLUSION

Security of the message is paramount during its transmission from one user to another user or system. A cryptographic technique provides a message security. Symmetric-key cryptography is very good in providing security to the message but suffers from key distribution and management problems. We have compare both RSA and ECC based on the bits size on three sample input data of 8 bits, 64 bits, 256 bits by using python programming and we plotted the graph to show the comparison in time lapse on encyption and decryption.

References

[1] Batina, L., Mentens, N., Sakiyama, K., Preneel, B., and Verbauwhed, I., Public- Key Cryptography on the Top of Niddle, https://www.researchgate.net/publication/221381449, (2007), 1831-1834.

[2] J.A. Buchmann, Introduction to Cryptography, Second Edition, Springer, (2008)

[3] Kapoor, V. , Abraham, V.S., and Singh, R., Elliptic curve cryptography, Ubiquity (ACM, New York, NY, USA), 2008 (2008), 1-8.

[4] Liestyuwati, B., Public Key Cryptography, *J*ournal of physics (conference series), 1477 052062, (2020), 1-7.

[5] Sahinaslan.E,Sahinaslan.O,Cryptographic Methods and Development Stages Used Throughout History,AIP Conference Proceedings 2086, 030033 (2019),1-3

[6] Mahto, D., And Yadav, D.K., RSA and ECC : A comparative analysis, International Journal of applied engineering research, 12(19) (2017), 9053-9061.

[7] Mahto, D., And Yadav D. K., Performance Analysis of RSA and Elliptic Curve Cryptography, International Journal of Netw. Secur., 20(4) (2018), 625-635.

[8] Raju, GVS and Akbani, R., Elliptic curve cryptosystem and it's applications, SMC'03 Conference Proceedings (IEEE International Conference on Systems, Man and Cybernetics), 2 (2003), 1540-1543.

[9] The Code Book. The secret History of codes and codes-breaking,Simon Singh,(1999)

[10] Vigila, S.M.C., and Muneeswaran, k., Implementation of text based cryptosystem using elliptic curve cryptography, First International Conference on Advanced Computing (IEEE), (2009), 82-85.

[11] W.stallings, Cryptography and Network security, 5th ed. Boston: Prentice Hall,(2011)